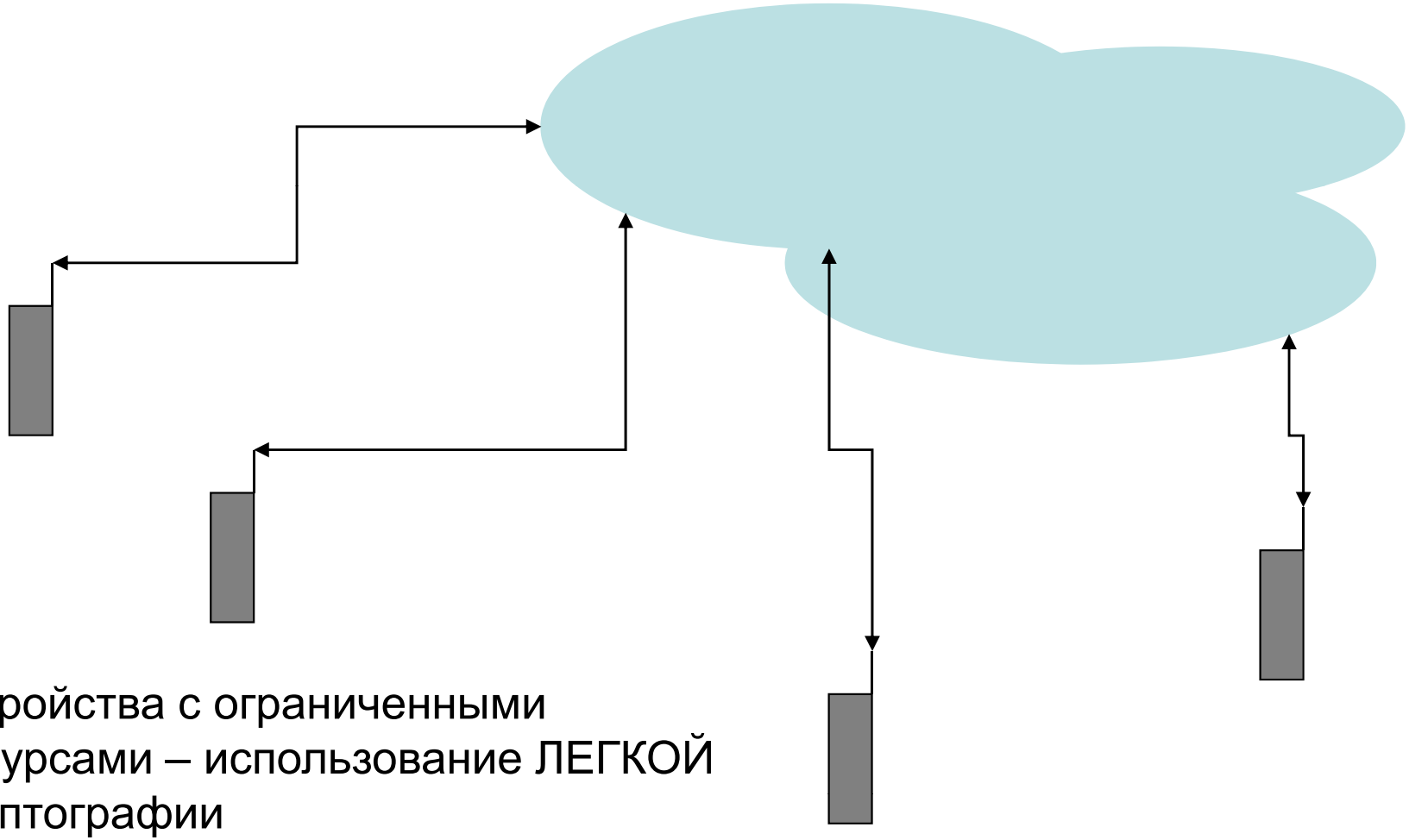
Использование кодовых методов для решения задач информационной безопасности в облачных системах хранения и обработки данных

Крук Евгений Аврамович,
д.т.н., проф.,
Беззатеев Сергей Валентинович,
д.т.н. , доц.,

Санкт Петербургский Государственный
Университет Аэрокосмического
Приборостроения

РусКрипто’ 2012

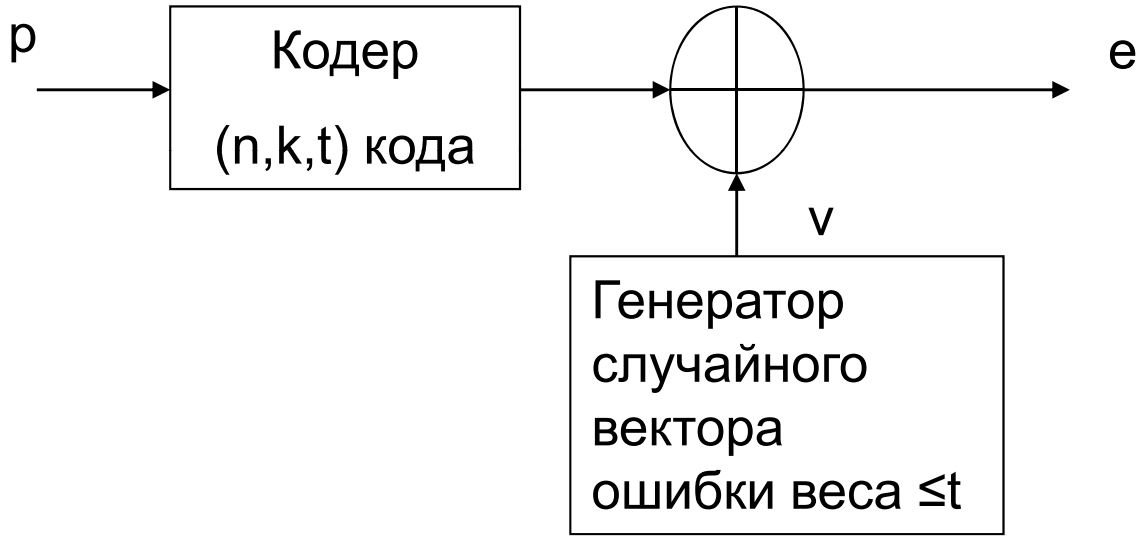
Облачные системы



Устройства с ограниченными ресурсами – использование ЛЕГКОЙ криптографии

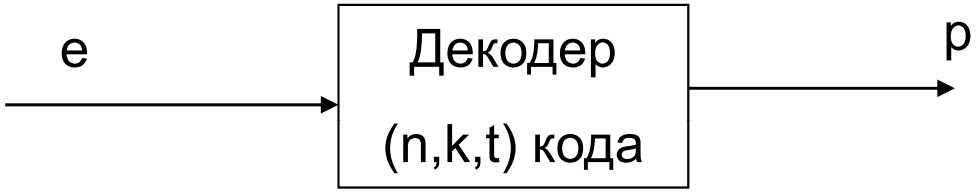
Основные примитивы кодовой криптографии

Шифрация



Ключ – знание алгоритма декодирования (n,k,t) кода

Дешифрация



Шифрация/Дешифрация

(n,k,t) код с порождающей матрицей **G** [*k*×*n*],

P – перестановочная матрица [*n*×*n*],

A – обратимая матрица [*k*×*k*],

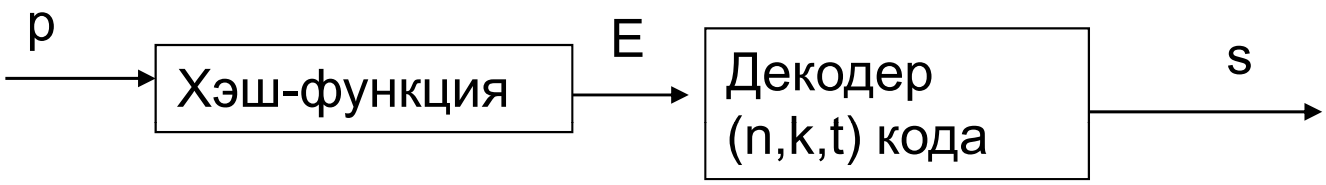
A×G×P =O – открытый ключ.

Шифрация: ***p*×O+*v* = *e*,**

Дешифрация: декодирование вектора ***e*** при знании ***(n,k,t)*** кода с исправлением вектора ошибки ***v***.

Основные примитивы кодовой криптографии

Подпись



Ключ – знание алгоритма декодирования (n,k,t) кода

Проверка

Подпись/проверка

(n,k,t) код с проверочной матрицей **H** [*r*×*n*],

P – перестановочная матрица [*n*×*n*],

A – обратимая матрица [*r*×*r*], *r=n-k,*

A×H×P =O – открытый ключ.

E = Hash(**p**)

Декодирование **E** при знании (***n,k,t***) кода,

получение подписи(вектора ошибки)***s*** :

$\boldsymbol{s \times O^T = E}$

Проверка подписи: Hash(**p**)= $\mathbf{E} \stackrel{?}{=} \boldsymbol{s} \times \mathbf{O}^{\mathbf{T}}$

Основные особенности алгоритма шифрации/дешифрации

Быстрота

- Шифрация : 140-200 Mb/c (120-170 циклов/байт)
- Дешифрация: 20-90 Mb/c (300-1300 циклов/байт)
  - По сравнению с RSA: шифрация *×1/ 5*, дешифрация от × 1/20 *до* *×1/*100

***Большой открытый ключ*: от 10 до 30 Кб**

- По сравнению с RSA: от ×10 до ×30

Безопасность

- Сложность декодирования случайного (n,k,t) кода
- Псевдослучайность (n,k,t) кодов Гоппы
- Устойчивость к квантовым вычислениям

Сравнительные характеристики

$(m;t)$	$n=2^m$	k	t	ключ (Кбайт)	Шифрация (цикл/байт)	Дешифрация (цикл/байт)	Безопасность сообщения($\log_2$)	Безопасность ключа ($\log_2$)
(10;50)	1024	524	50	32	243	7938	60	491
(11;32)	2048	1696	32	73	178	1848	88	344
(12;21)	4096	3844	21	118	125	573	88	244
(13;17)	8192	7971	17	215	119	312	89	213
(12;40)	4096	3616	40	212	180	1016	128	471
(13;29)	8192	7815	29	360	139	434	129	368

	Шифрация (цикл/байт)	Дешифрация (цикл/байт)
RSA1024	800	23100
RSA2048	834	55922
NTRU	4753	8445

N. Sendrier, On the Key Security of Code-based Public-key Cryptosystems, PQSM'10, Paris, 2010

Проблемы конфиденциальности

- Разграничение доступа пользователей в зависимости от их уровня, то есть задача распределения ключей

Использование семейств вложенных кодов $(n,k_1,t_1) \subset (n,k_2,t_2) \subset \ldots \subset (n,k_i,t_i)$

(шифрация, дешифрация)

Целостность и аутентификация

- Аутентификация сообщений

  (подпись)

- Протоколы аутентификации

  (шифрация.дешифрация)

Проблемы анонимности

- Анонимность пользователя

  – Слепая подпись

    (подпись)

Проблемы анонимности

- Анонимность запроса к данным

Использование семейств кодов

$\{(n,k_1,t_1)\ ,\ (n,k_2,t_2)\ ,\ \ldots\ \} \subset (n,k_i,t_i)$

(шифрация.дешифрация)

Проблемы анонимности

- Анонимность источника запроса

  Onion – протокол

  (шифрация.дешифрация)

СПАСИБО

ЗА

ВНИМАНИЕ!

Сравнительные характеристики

n, k, t	Открытый ключ (байты)	Шифрация $\log_2$(бинарных операций на блок)	Дешифрация $\log_2$(бинарных операций на блок)	Безопасность сообщения $\log_2$
(1024,524,50)	67072	9	13.25	65
RSA362	46	17	17	68
(2048,1025,93)	262400	10	14.5	107
RSA1024	256	20	20	110
RSA2048	512	22	22	145
(4096,2056,170)	1052672	11	15.5	187
RSA4096	1024	24	24	194

D. B. Ojha, A.Sharma, A. Dwivedi,N.Pandey,A. Kumar, An Approach for Secure Transmission of Large Medical Data Using Post Quantum Cryptosystem Advances in Computational Sciences and Technology, ISSN 0973-6107, V. 4, N, 1 (2011) pp. 73–81

Литература

- 1. Беззатеев С.В., Многоуровневая система разграничения доступа на схеме Мак Элиса, Проблемы информационной безопасности. Компьютерные системы, 2010, №3, с.42-44.
- 2. Loureiro S., Molva R., Function hiding based on error correcting codes, Proceedings of Cryptec'99, pp. 92-98, City University of Hong-Kong, July 1999.
- 3. G. Kabatianskii, E. Krouk and B. Smeets, A digital signature scheme based on random error–correcting codes, the 6th IMA International Conference Cirencester, UK, December 1997, pp.161–177.
- 4. Woo-Hun Kim, Eun-Jun Yoon and Kee-Young Yoo, New Authentication Protocol Providing User Anonymity in Open Network , Lecture Notes in Computer Science, 2005, v. 3828/2005, pp. 414-423,
- 5. Беззатеев С.В., Коды Гоппы в протоколах анонимного запроса к данным, Информационноуправляющие системы , 2010, №6, с.86-87.